Vulnérabilité des systèmes d'information

Type de contenu : Texte

Titre(s) : Vulnérabilité des systèmes d'information [texte imprimé] : découverte, exploitation et perspectives / enseigne de vaisseau Erulin Régis ; organisme d'accueil Naval Group ; tuteur de projet : M. Hébrard, responsable recherche et innovation cyber chez Naval Group

Auteur(s) : Erulin, Régis EN2015

Editeur, producteur : Lanvéoc-Poulmic : Ecole navale, 2017

Description matérielle : 1 vol. (X-39 p.) : ill. en noir et en coul. ; 30 cm

Note de thèses et écrits académiques : PFE Systèmes informatiques et modélisation 2017 Ecole navale

Résumé ou extrait : Notre projet s'est déroulé au sein du Laboratoire de Cybersécurité navale, situé sur le site d'Ollioules de Naval Group. Nous y avons réalisé un pentest sur un réseau informatique simulé, afin d'étudier le processus qui mène à une cyberattaque, du choix de la cible aux actions finales sur celles-ci. Dans ce cadre, nous étudions dans ce rapport le concept de vulnérabilité informatique et les méthodes générales pour l'exploitation de celles-ci, notamment la cyber kill chain, et les différents types et objectifs d'attaques, plus particulièrement les APT. Nous passons dans un second temps à l'étude de cas concrets, avec la description d'une attaque récemment intervenue sur des sites d'Etat, avant de décrire notre propre attaque, segmentée en étapes correspondant aux systèmes dont nous prenons le contrôle. Dans un troisième temps, nous étudions les contre-mesures et protections possibles en nous axant sur les 5 piliers du NIST Cyber Security Framework, que sont l'identification des menaces, la protection contre ces menaces, la détection des attaques, la réaction à ces attaques, et la réparation des dégâts causés par ces attaques. En conclusion, nous donnons un état actuel de différentes initiatives de cyberdéfense visant à rendre celle-ci plus efficace et mieux coordonnée, afin de contrer une menace toujours grandissante.